REMARKS

Reconsideration of the present application is requested.

Applicants acknowledge the withdrawal of claims 5, 8-10, 12-13 and 33-40. Claims 1-2, 6-7, 14 and 22-32 are currently under examination.

Objections to the Specification

The Office Action includes an objection to the specification because "computer-readable storage medium" in claims 14 and 23 allegedly lacks antecedent basis in the specification. Applicants fail to understand this objection being that there is no *in haec verba* requirement for the specification. See, MPEP § 2163. That is, an explicit recitation of "computer-readable storage medium" need not be set forth in the specification. Throughout the specification, the term "storage medium" is used. In the context of the present application, one of ordinary skill would surely appreciate that "storage medium" in the specification is indeed a "computer-readable storage medium." For at least this reason, withdrawal of this objection is requested.

Claim Objections

Claims 1-2, 6-7, 14 and 32 stand objected to due to minor informalities. Although Applicants do not necessarily agree with each of the Examiner's

objections. Applicants have amended the claims where necessary taking into account the Examiner's comments. Withdrawal of this objection is requested.

Rejections under 35 U.S.C. § 101

Claims 1-2, 6-7, 14, 22-30 and 32 stand rejected under 35 U.S.C. § 101 as being directed to nonstatutory subject matter. Although Applicants do not necessarily agree with the Examiner's rejection, Applicants have amended claim 1 taking into account the Examiner's comments. As amended. claim 1 recites:

> performing, by a security check device, a security check to ascertain a user identity by comparing entered identity information with stored user identity data: [...]
>
> performing, by at least one processor, at least one of encrypting and decrypting data using the acquired at least one data key and inhibiting user recognition of the acquired at least one data key.

Thus, claim 1 is positively tied to a particular machine; namely a security check device and/or at least one processor. Claim 22 has been amended in a manner similar to claim 1. Therefore, withdrawal of this rejection is requested.

Rejections under 35 U.S.C. § 103

Claims 1, 2, 6, 7, 14, and 22-32 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent No. 6,031,910 ("Deindl") in view of U.S. Patent No. 7,272,230 ("Sasaki"). This rejection is respectfully traversed.[1]

Deindl discloses a method for storing information on at least one storage medium with the aid of a chip card. According to column 6, lines 22-43, a chip card generates a first cryptographic key, which is transmitted to a computer. Using the transmitted first cryptographic key, the computer encrypts data to be stored on the storage medium. Within the chip card, the transmitted first cryptographic key is encrypted with a second cryptographic key, which is not provided to the computer. Both the encrypted data and the encrypted key are stored on the storage medium.

At page 7, the Office Action directs Applicants' attention to the "personal identification number, a password and/or biometric identification – e.g. col. 6, lines 37-39" of Deindl to disclose the claimed "user identifier." Contrary to claim 1, however, these forms of identification are entered by the user, not stored in a first data store as is the case with the "user identifier" of claim 1.

---

[1] To be thorough, further expedite prosecution, and for the sake of clarity, Applicants provide discussions of each of the references separately, however, Applicants are not attacking these references individually, but arguing that the references, even taken in combination, fail to render the claimed invention obvious because all features of claim 1 are not found in the prior art.

Further, Deindl does not disclose or fairly suggest any associating of these identifications with a user identity.

As the Examiner will appreciate, claim 1 requires both a "user identity" and a "user identifier" as well as associating the two together. The user identity is ascertained by comparing *entered identity information with stored user identity data.* The ascertained user identity is then *associated with* a user identifier stored in a first data store. At best, the personal identification number, password and/or biometric identification mentioned in Deindl are identity information entered by a user, but not a "user identity" or "user identifier."

Therefore, Deindl fails to disclose or fairly suggest at least "*associating the user identity with a user identifier stored in a first data store*" as required by claim 1.

Further, at page 7, the Office Action directs Applicants' attention to column 6, lines 22-23 and 44-56 to disclose "*associating the user identifier with at least one user group identifier*" as required by claim 1. Applicants disagree because Deindl does not disclose or fairly suggest actively associating a user identifier with at least one user group identifier stored in a second data store.

Specifically, at column 6, lines 22-23 Deindl merely discloses that a user is assigned to a group. Further, at column 6, lines 44-56, Deindl states in-part:

In an embodiment, the method further includes the step of producing a data header in the computer for each of a plurality of data records, where the data header indicates to which of a plurality of user groups a particular user that is writing belongs to...

Neither portion of Deindl, however, discloses a second data store in which a user group identifier is stored. Further, neither portion of Deindl discloses an active association between the user identifier and user group identifier. At best, lines 44-56 in column 6 of Deindl disclose generating a data header, which identifies the user group to which the particular user belongs. Therefore, Deindl also fails to disclose or suggest "*associating the user identifier with at least one user group identifier stored in a second data store*" as required by claim 1.

Moving forward, as correctly recognized by the Examiner, Deindl does not disclose or fairly suggest at least a centralized third data store including all available keys. The Office Action, at pages 7 and 8 directs Applicants' attention to Sasaki to disclose this feature. Particularly, the Office Action refers to the second management database 16 in FIG. 31 of Sasaki to disclose the centralized third data store of claim 1.

Sasaki discloses an encryption system and method. FIG. 31 of Sasaki shows a second management database 16. The second management database 16 includes a group key and a group ID. The group ID identifies the group to which a user of the cryptographic system belongs. The group key is a random

number data given for each of the groups. But, Sasaki suffers from at least the

same deficiencies as Deindl with respect to claim 1. Namely, Sasaki fails to

disclose or suggest at least "*associating the user identity with a user identifier*

stored in a first data store" and "*associating the user identifier with at least one*

user group identifier stored in a second data store."

Because neither Deindl nor Sasaki discloses or suggests the associating

steps required by claim 1, Deindl in view of Sasaki (assuming *arguendo* that

the references could be combined, which Applicants do not admit) fails to

render claim 1 obvious.

In addition, amended claim 1 requires, *inter alia*, three data stores, a first

of which stores a user identifier, a second of which stores a group identifier and

a third of which stores data keys. Neither Deindl nor Sasaki, taken singly or in

combination, discloses such a modular structure. Therefore, the references fail

to render claim 1 obvious.

Claims 22 and 31 recite at least some features similar to those set forth

in claim 1. Therefore, claims 22 and 31 are patentable over Deindl in view of

Sasaki for at least somewhat similar reasons.

Deindl in view of Sasaki fails to render claims 2, 6, 7, 14, and 23-30 and

32 obvious at least by virtue of their dependency from claim 1. Withdrawal of

this rejection is requested.

Attorney Docket No: 32860-000704/US
Application No. 10/785,180
Page 17

CONCLUSION

In view of above remarks, reconsideration of the outstanding rejection and allowance of the pending claims is respectfully requested.

If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone Andrew M. Waxman, Reg. No. 56,007, at the number listed below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY & PIERCE, PLC

By _____ 56,007

Donald J. Daley
Reg. No. 35,313

DJD/AMW:clc

P.O. Box 8910
Reston, VA 20195
(703) 668-8000